أمن المعلومات

GS224 - 9

اصناف المتسللين: المجرمين

- الأفراد أو أعضاء جماعة الجريمة المنظمة بهدف الحصول على مكافأة مالية
  - لصوص الهوية
  - لصوص أوراق الاعتماد المالية
  - التجسس على أسرار الشركات
  - لصوص البيانات
  - فدية البيانات
- عادةً ما يكونوا متسللين صغارًا ، وممن يمارسون أعمالهم على الويب.
- يجتمعون في منتديات سرية لتبادل النصائح والبيانات وتنسيق الهجمات.

اصناف المتسللين: النشطاء

- هم إما أفراد يعملون عادةً كمخبرين ، أو أعضاء في مجموعة أكبر من المهاجمين الخارجيين بدوافع اجتماعية أو سياسية
- تعرف أيضًا باسم نشطاء القرصنة
  - غالبًا ما يكون مستوى مهارتهم منخفضًا
- غالبًا ما يكون الهدف من هجماتهم هو الترويج لقضيتهم والإعلان عنها من خلال:
  - تشويه الموقع
  - هجمات رفض الخدمة
  - سرقة البيانات وتوزيعها مما يؤدي إلى دعاية سلبية أو المساومة على أهدافهم

اصناف المتسللين: الدخلاء - برعاية الدولة

- مجموعات قراصنة ترعاها الحكومات للقيام بأنشطة تجسس أو تخريب.
- تُعرف أيضًا بالتهديدات المستمرة المتقدمة (APTs) نظرًا لطبيعتها السرية والمثابرة و الاستمرارية على مدى فترات طويلة المرتبطة بأي هجمات من هذه الفئة.
- طبيعة ونطاق واسع النطاق لهذه الأنشطة من قبل مجموعة واسعة من البلدان من الصين إلى روسيا والولايات المتحدة الأمريكية والمملكة المتحدة وحلفائهم الاستخباراتيين.

اصناف المتسللين: اخرون

- قراصنة بدوافع غير تلك المذكورة سابقًا.
- تتضمن المتسللين الكلاسيكيين أو المخترقين الذين يحركهم التحدي التقني أو التقدير والسمعة من الأقران.
- يمكن اعتبارهم مسؤولين عن اكتشاف فئات جديدة من الثغرات.
- نظرًا للتوفر الواسع لمجموعات أدوات الهجوم ، هناك مجموعة من "المتسللين الهواة" الذين يستخدمونها لاستكشاف أمان النظام والشبكة.

مستوى المهارة: مبتدئ

- قراصنة يتمتعون بأقل قدر من المهارات التقنية ويستخدمون بشكل أساسي أدوات الهجوم المتوفرة حاليا.
- ربما يشكلون أكبر عدد من المهاجمين ، بما في ذلك العديد من المجرمين والنشطاء المهاجمين.
- نظرًا لاستخدامهم للأدوات المعروفة والموجودة حاليا، فإن هؤلاء المهاجمين هم الأسهل للدفاع ضدهم.
- يُعرفون أيضًا باسم " كتاب طفوليين" (script-kiddies) نظرًا لاستخدامهم للنصوص البرمجية الموجودة (الأدوات).

مستوى المهارة: بارع

- قراصنة يتمتعون بمهارات تقنية كافية لتعديل مجموعات أدوات الهجوم المعروفة وتوسيع نطاقها لاستخدام نقاط ضعف مكتشفة أو مشتراة حديثًا.
- قد يكونون قادرين على تحديد نقاط الضعف الجديدة ويمكن استغلالها وتشبه بعض الثغرات المعروفة.
- من المحتمل وجود قراصنة بهذه المهارات في جميع فئات المتسللين.
- تكييف الأدوات لاستخدامها من قبل اخرين.

مستوى المهارة: خبير

- قراصنة يتمتعون بمهارات تقنية عالية المستوى وقادرون على اكتشاف فئات جديدة من نقاط الضعف.
- يكتبون مجموعة أدوات (برمجيات تطبيقية) هجوم قوية وجديدة.
- بعض المتسللين الكلاسيكيين المعروفين هم من هذا المستوى.
- يتم توظيف البعض من قبل المنظمات التي ترعاها الدولة.
- الدفاع ضد هذه الهجمات هو الأكثر صعوبة.

المتسللين: تصنيفات اخرى

- متنكر: الأفراد غير المصرح لهم ويخترقون النظام.
- مستاء: مستخدم شرعي يصل إلى بيانات غير مصرح بها.
- سري: يستولي على تحكم المشرف.

التعدي على المستخدمين والبرمجيات

- تعدي على المستخدم: تسجيل الدخول غير المصرح به ، وإساءة استخدام الامتيازات.
- التعدي على البرنامج: فيروس أو دودة أو حصان طروادة .

امثلة على التطفل

- اختراق عن بعدد لخادم البريد الإلكتروني
- تشويه خادم الويب
- التخمين وتكسير كلمات المرور
- نسخ قاعدة بيانات تحتوي على أرقام بطاقات الائتمان
- عرض البيانات الحساسة ، بما في ذلك سجلات الرواتب والمعلومات الطبية بدون إذن
- تنفيذ حزمة تشمم على محطة عمل لالتقاط أسماء المستخدمين وكلمات المرور
- استخدام خادم (FTP) مجهول لتوزيع البرامج المقرصنة وملفات الموسيقى
- الاتصال بمودم غير آمن والحصول على وصول داخلي للشبكة
- التظاهر كمشرف تنفيذي والاتصال بمكتب المساعدة ، وإعادة تعيين كلمة المرور البريد الإلكتروني للمدير التنفيذي، وتعلم كلمة المرور الجديدة
- استخدام محطة عمل غير مراقبة تم تسجيل دخولها بدون إذن

سلوك المتطفل

- بهدف الاستحواذ وجمع المعلومات
- الوصول أولا للنظام
- تطوير الامتيازات
- جمع المعلومات أو استغلال النظام
- المحافظة على الوصول للنظام
- السيطرة على المسارات

مثال على سلوك القراصنة

- تحديد الهدف باستخدام أدوات بحث (IP)
- استعراض الشبكة لاستكشاف الخدمات التي يمكن الوصول إليها
  - دراسة الاتصال المادي عبر بروتوكول (NMAP)
- تحديد الخدمات التي يحتمل أن تكون عرضة للضعف
- تخمين كلمات مرور (القوة التحليلية)
- تثبيت أداة اشراف عن بعد
- انتظر حتى يقوم المشرف بتسجيل الدخول والتقاط كلمة المرور
- استخدم كلمة المرور للوصول إلى باقي الشبكة

مثال على سلوك القراصنة

تتغير تقنيات وأنماط سلوك المتسللين باستمرار لاستغلال نقاط الضعف المكتشفة حديثًا والتهرب من الاكتشاف والتدابير المضادة. ومع ذلك ، فإن المتسللين عادةً ما يتبعون واحدًا من عدد من أنماط السلوك التي يمكن التعرف عليها ، وتختلف هذه الأنماط عادةً عن تلك الخاصة بالمستخدمين العاديين.

مثال: اقتحام لمؤسسة مالية كبيرة. استغل الدخيل حقيقة أن شبكة الشركة كانت تشغل خدمات غير محمية ، وبعضها لم تكن هناك حاجة له. في هذه الحالة ، كان مفتاح الاختراق هو تطبيق حاسوب " pc Anywhere". تعلن الشركة المصنعة (Symantec) عن هذا البرنامج كحل للتحكم عن بعد يتيح الاتصال الآمن بالأجهزة البعيدة. لكن المهاجم كان لديه وقت سهل للوصول إلى جهاز الحاسوب من أي مكان ؛ استخدم المسؤول نفس اسم المستخدم وكلمة المرور المكونين من ثلاثة أحرف للبرنامج. في هذه الحالة ، لم يكن هناك نظام للكشف عن التسلل على شبكة الشركة المكونة من 700 عقدة. تم اكتشاف الدخيل فقط عندما دخلت نائبة الرئيس إلى مكتبها ورأت المؤشر يحرك الملفات على محطة عمل ويندوز الخاصة بها.

سلوك المتسلل المجرم

- يتصرفون بسرعة وبدقة لجعل اكتشاف أنشطتهم أكثر صعوبة
- استغلال المحيط عبر المنافذ الضعيفة
- استخدم أحصنة طروادة (برنامج مخفي) لترك الأبواب الخلفية للدخول مرة أخرى
- استخدم التشمم لالتقاط كلمات المرور
- لا تبقى حتى لا تلاحظ
- ارتكب القليل من الأخطاء أو لا ترتكب أي أخطاء

سلوك المتسللين المخبرين

- إنشاء حسابات شبكة لأنفسهم ولأصدقائهم
- الوصول إلى الحسابات والتطبيقات التي لا يستخدمونها عادةً في وظائفهم اليومية
- البريد الإلكتروني لأصحاب العمل السابقين والمحتملين
- إجراء محادثات مراسلة فورية سرية (سرا)
- يقوم بزيارة مواقع الويب التي تلبي احتياجات الموظفين الساخطين .
- يقوم بإجراء تنزيلات كبيرة ونسخ الملفات
- الوصول إلى الشبكة في غير أوقات الدوام

هجوم المخبرين

- من بين الأكثر صعوبة في الكشف والمنع
- يمتلك الموظفون قدرة الوصول ومعرفة بالأنظمة
- قد يكون الدافع هو الانتقام / السخط
  - عند إنهاء العمل
  - بيانات العميل عند الانتقال إلى منافس
- قد تساعد أنظمة كشف الاختراق

هجوم المخبرين : مثال

تعتبر هجمات المخبرين من أكثر الهجمات التي يصعب اكتشافها ومنعها. يتمتع الموظفون بالفعل بإمكانية الوصول والمعرفة حول بنية قواعد بيانات الشركة ومحتواها. يمكن أن يكون الدافع وراء هجمات المخبرين هو الانتقام لمجرد الشعور بالسخط. مثال على السابق هو حالة كينيث باترسون ، الذي طرد من منصبه كمدير اتصالات البيانات لشركة (American Eagle Outfitters) عطّل باترسون قدرة الشركة على معالجة مشتريات بطاقات الائتمان خلال خمسة أيام من موسم العطلات لعام 2002. أما بالنسبة للشعور بالسخط ، فقد كان هناك دائمًا العديد من الموظفين الذين شعروا بحقهم في الحصول على لوازم مكتبية إضافية للاستخدام المنزلي ، ولكن هذا يمتد الآن إلى بيانات الشركة. مثال على ذلك نائبة رئيس المبيعات لشركة تحليل الأسهم التي استقالت للذهاب إلى منافس. قبل أن تغادر ، قامت بنسخ قاعدة بيانات العملاء لأخذها معها. ذكرت الجانية أنها لا تشعر بأي عداء تجاه موظفها السابق ؛ لقد أرادت البيانات لأنها ستكون مفيدة لها. على الرغم أن أنظمة منع الاختراق يمكن أن تكون مفيدة في مواجهة الهجمات الداخلية ، إلا أن اساليب الأخرى مباشرة لها أولوية أعلى. تتضمن الأمثلة: فرض الامتياز الأقل ، ومراقبة السجلات ، وحماية الموارد الحساسة بمصادقة قوية ، وعند الإنهاء ، احذف وصول الكمبيوتر والشبكة للموظف وعمل صورة معكوسة للقرص الصلب للموظف قبل إعادة إصداره.

التسلل والكشف الأمني

- التسلل الأمني: حدث أمني ، أو مجموعة من الأحداث الأمنية المتعددة ، والتي تشكل حادثًا أمنيًا يكتسب فيه متطفل ، أو يحاول الوصول إلى نظام (أو مورد نظام) دون الحصول على إذن للقيام بذلك.
- كشف الاختراق: خدمة أمنية تراقب وتحلل أحداث النظام بغرض البحث عن ، كذلك تقديم تحذير في الوقت الحقيقي أو شبه حقيقي لمحاولات الوصول إلى موارد النظام بطريقة غير مصرح بها.

تقنيات التسلل

- هدف المتسلل هو الوصول إلى نظام أو زيادة نطاق الامتيازات التي يمكن الوصول إليها على النظام.
- تستخدم معظم الهجمات الأولية ثغرات النظام أو البرامج التي تسمح للمستخدم بتنفيذ تعليمات برمجية تفتح بابًا خلفيًا للنظام.
- يمكن للمتسللين الوصول إلى نظام من خلال استغلال هجمات مثل فيض المخزن المؤقت (buffer overflows) على برنامج ينفذ بامتيازات معينة.
- يحاول المتسلل الحصول على معلومات كان يجب حمايتها. في بعض الحالات ، تكون هذه المعلومات في شكل كلمة مرور المستخدم. من خلال معرفة كلمة مرور مستخدم آخر ، يمكن للمتسلل تسجيل الدخول إلى النظام وممارسة جميع الامتيازات الممنوحة للمستخدم الشرعي.

أنظمة كشف التسلل (IDS)

- المستضافة (HIDS) : تراقب خصائص مضيف والأحداث التي تحدث داخل ذلك المضيف ، مثل معرفات العملية واستدعاءات التي يجريها النظام للحصول على دليل على نشاط مشبوه.
- الشبكية (NIDS) : تراقب حركة مرور الشبكة من اجل أجزاء او أجهزة معينة على الشبكة لتحليل بروتكولات الشبكة لتحديد ما اذا كان هناك النشاط المشبوه.
- أنظمة كشف التسلل الموزعة أو المختلطة: تجمع المعلومات من عدد من أجهزة الاستشعار ، غالبًا المعتمدة الأنظمة المستضافة والشبكية ، في محلل مركزي قادر على تحسين تحديد نشاط التسلل والاستجابة له.

مكونات أنظمة كشف التسلل (IDS)

- أجهزة الاستشعار: هي المسؤولة عن جمع البيانات. مدخلات جهاز الاستشعار قد يكون أي جزء من النظام يمكن أن يحتوي على دليل على التسلل. أنواع مدخلات جهاز الاستشعار يتضمن حزم الشبكة ، وملفات التسجيل ، ومتتبعات استدعاءات النظام. تقوم المستشعرات بجمع هذه المعلومات وإرسالها إلى المحلل.
- أجهزة التحليل: تتلقى أجهزة التحليل المدخلات من جهاز استشعار واحد أو أكثر أو من أجهزة محللات اخرى. المحلل مسؤول عن تحديد ما إذا كان التسلل حدث أم لا ، يخرج إشارة إلى حدوث اقتحام او تسلل. وقد تتضمن المخرجات أدلة تدعم الاستنتاج بحدوث ذلك التسلل. قد يوفر المحلل إرشادات حول ماهى الإجراءات التي يجب ان تتخذ نتيجة هذا التسلل. يمكن أيضًا تخزين مدخلات المستشعر للتحليل والمراجعة في المستقبل في قاعدة للبيانات.
- واجهة المستخدم: تتيح واجهة المستخدم لنظام كشف التسلل للمستخدم إمكانية عرض المخرجات من النظام أو التحكم في سلوك النظام. في بعض الأنظمة ، واجهة المستخدم تناسب المدير أو المشرف أو وحدة تحكم.

مبادئ أنظمة كشف التسلل (IDS)

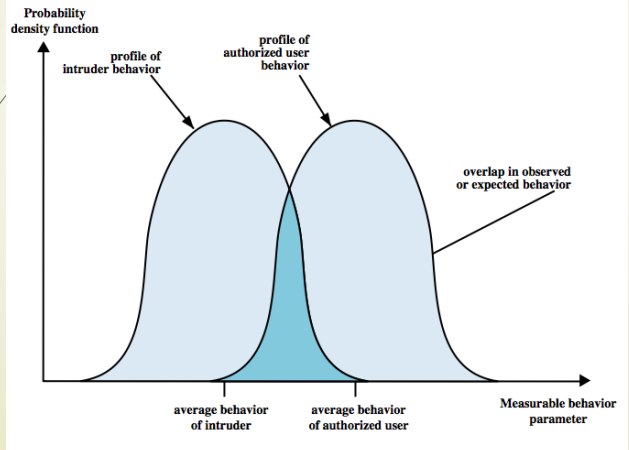
- يعتمد كشف التسلل على افتراض أن سلوك المتسلل يختلف عن سلوك المستخدم الشرعي بطرق يمكن قياسها كمياً. بالطبع ، لا يمكننا أن نتوقع أنه سيكون هناك تمييز دقيق ودقيق بين هجوم من قبل متسلل والاستخدام العادي للموارد من قبل مستخدم مصرح له. بدلاً من ذلك ، يجب أن نتوقع أنه سيكون هناك بعض التداخل ، كما هو موضح في الشكل . يمكن تحديد أنماط السلوك الشرعي للمستخدم من خلال مراقبة التاريخ الماضي ، ويمكن اكتشاف انحراف كبير عن هذه الأنماط. على الرغم من أن السلوك النموذجي للمتسلل يختلف عن السلوك المعتاد للمستخدم المصرح له ، إلا أن هناك تداخلًا في هذه السلوكيات. وبالتالي ، فإن التفسير الفضفاض لسلوك المتسلل سيصطاد المزيد من المتسللين ، سيؤدي أيضًا إلى عدد من الإيجابيات الكاذبة ، أو المستخدمين المصرح لهم الذين تم تحديدهم على أنهم متسللون. من ناحية أخرى ، ستؤدي محاولة الحد من الإيجابيات الكاذبة من خلال التفسير الدقيق لسلوك الدخيل إلى زيادة السلبيات الكاذبة أو المتسللين الذين لم يتم تحديدهم على أنهم متسللون. وبالتالي ، هناك عنصر حل وسط وفن في ممارسة كشف التسلل.

مبادئ أنظمة كشف التسلل (IDS)

loose vs tight interpretation:
catch more (false +) or catch less (false -)

valid user identified as intruder

intruder not identified



متطلبات أنظمة كشف التسلل (IDS)

نظام كشف التسلل يجب:

- يعمل باستمرار بأدنى حد من الإشراف البشري.
- يكون متسهلا مع الأخطاء بمعنى أنه يجب أن يكون قادرًا على التعافي من أعطال النظام وإعادة التهيئة.
- مقاومة للتخريب ، حيث يجب أن يكون نظام كشف التسلل قادرًا على مراقبة نفسه واكتشاف ما إذا كان قد تم تعديله بواسطة مهاجم.
- فرض حد أدنى من الاجهاد على النظام عند تشغيله.
- أن يكون قادرا على التهيئة وفقًا لسياسات الأمن للنظام الذي تتم مراقبته.
- ان يكون قادرا على التكيف مع التغييرات في النظام وسلوك المستخدم بمرور الوقت.
- ان يكون قادرا على التوسع لمراقبة عدد كبير من المضيفين.
- توفير تدهور سلس للخدمة بمعنى أنه إذا توقفت بعض مكونات نظام كشف التسلل عن العمل لأي سبب من الأسباب ، فيجب أن لا يتأثر الباقي.
- السماح بإعادة التكوين الديناميكي ، أي القدرة على إعادة تكوين نظام كشف التسلل دون الحاجة إلى إعادة تشغيله.

أنظمة كشف التسلل : تقنيات الكشف

- كشف السلوك الغريب: يتضمن جمع البيانات المتعلقة بالسلوك من المستخدمين الشرعيين على مدار فترة زمنية. ثم السلوك الحالي المرصود هو تم تحليلها لتحديد مستوى عالٍ من الثقة فيما إذا كان هذا السلوك أم لا مستخدم شرعي أو متسلل.
- الكشف الاسترشادي : يستخدم مجموعة من أنماط البيانات الخبيثة المعروفة (التوقيعات) أو قواعد الهجوم (الاستدلال) التي تتم مقارنتها بالسلوك الحالي أو لتقرير ما إذا كان متسللا ام لا. يُعرف أيضًا باسم اكتشاف إساءة الاستخدام. هذه النهج يمكنه فقط تحديد الهجمات المعروفة التي لها أنماط أو قواعد.